FEDERAL EXECUTIVE BOARD

# Chicago Federal Information Technology Council

3CPO

CHICAGO COORDINATED CONTINGENCY PLANNING OPERATION for IT Systems

# The Chicago Coordinated Contingency Planning Operation for IT Systems

## *Introduction*

Information Technology (IT) systems are vulnerable to a variety of disruptions, ranging from mild (e.g., short-term power outage, disk drive failure) to severe (e.g., equipment destruction, fire) from a variety of sources such as natural disasters to terrorists actions. Much vulnerability can be minimized or eliminated through technical, management or operational solutions as part of the organization's risk management effort. Some vulnerability to critical resources resides outside the organization's control (such as electric power or telecommunications), and the organization may be unable to ensure their availability. Effective contingency planning, execution, and testing are essential to mitigate the risk of system and service unavailability.

## *Background*

In March 2002 the Chicago Federal Executive Board, with the Regional Offices of FEMA and GSA, conducted a COOP (Continuity of Operations Plan) Workshop. A COOP focuses on restoring an organization's essential functions at an alternate site and performing those functions for up to 30 days before returning to normal operations.

Because the COOP emphasizes the recovery of an organization's operational capability at an alternate site, the plan does not necessarily include IT operations. In addition, minor disruptions to IT systems or capabilities that do not require relocation to an alternate site are typically not addressed.

The Chicago Federal IT Council sees the need to build upon the FEB/FEMA/GSA COOP Workshop, to develop a coordinated contingency planning effort for IT systems and capabilities. The regional offices of many Federal agencies and departments in the Chicago area have insufficient IT staffs to plan, maintain and test effective contingency plans. In addition, many have limited local budgetary resources to obtain short-term commercially available alternative site strategies. Alternatively, some local agency and department facilities have extensive experience in these areas that should be shared. Some facilities are capable of providing short-term facilities, services and assistance. A coordinating effort is needed to assist agencies and departments to develop their IT system contingency plan, to determine their short-term recovery needs, and to suggest options for commercial resources or the identification of a ***Federal Contingency Partner*** agency.

## *Goals*

The ***Chicago Coordinated Contingency Planning Operation for IT Systems*** (hereinafter referred to as **3CPO**) was established to address the issues expressed above. The goal of **3CPO** is to pull together available resources and expertise within the Chicago Federal community to assist agency/department IT management in the following:

1. Understand the local IT Contingency Planning Process and its place within their overall headquarter-level Continuity of Operations Plan and Business Continuity Plan process.
2. Develop or reexamine the local contingency policy and planning process as an integral part of their overall headquarter-level process and apply the elements of the planning cycle, including preliminary planning, business impact analysis, alternate site selection, and recovery strategies.

3. Develop or reexamine the local application of their headquarter-level guidance on IT contingency planning policies and plans, with emphasis on maintenance, training and exercising the contingency plan.

**3CPO** will emphasize the need for Chicago regional organizations to build upon their headquarter-level plans to bring the contingency planning efforts down to a workable regional level.

**3CPO** will work with those agencies (GSA, FEMA, CIAO, NIST) with responsibilities and/or expertise in IT contingency planning to accomplish its goal in a variety of ways, including:

- Sponsor seminars based on NIST Special Publication 800-34, *Contingency Planning Guide for Information Technology Systems*.
- Conduct "discovery" sessions to inventory IT facility resource capabilities at Federal installations in the Chicago area, leading to the identification of ***Federal Contingency Partners***, including developing a sample Memorandum of Understanding and/or Interagency Agreement.
- Develop a local resource list of individuals with experience in the various aspects of IT contingency planning who are willing to share their knowledge and advice.
- Sponsor practical **Activation Workshops** on the process agencies/departments should take to notify recovery personnel and how to perform a damage assessment.
- Sponsor practical **Recovery Workshops** to provide guidance to agencies/departments in identifying potential courses of action for recovery teams and personnel to restore IT operations in the Chicago area at a ***Federal Contingency Partner*** location, a commercial facility, or using in-house contingency capabilities.
- Sponsor practical **Reconstitution Workshops** to outline actions agencies/departments should take to return their system to normal operating conditions.

***Keys to Success***

Vital elements to the success of **3CPO** include:

- The support of agency/department central offices, as well as Chicago regional office heads.
- Active participation of agencies such as NIST, CIAO, GSA, FEMA and others involved in areas of IT system contingency planning and homeland security.
- Cooperation in the identification of available IT resources and the development of interagency agreements for resource sharing in times of disaster.

## *IT Contingency Plan Local Implementation Evaluation Checklist*

| **Requirement (*Source*: *NIST SP 800-34*)** | **Local Implementation** | | | **Evaluation/Comments** |
|---|---|---|---|---|
| | **Full** | **Partial** | **Missing** | |
| ***Local Planning Process*** | | | | |
| 1. The IT contingency plan is based on a clearly defined policy and documented in a policy statement that describes the agency's overall contingency objectives, and establishes the organizational framework and responsibilities for local IT planning. | | | | |
| 2. The local IT contingency planning contains the following key elements:<br>▪ Roles and responsibilities,<br>▪ Scope as applies to the type(s) of platform(s) and organization functions subject to contingency planning,<br>▪ Resource requirements,<br>▪ Training requirements,<br>▪ Exercise and testing schedules,<br>▪ Plan maintenance schedule,<br>▪ Frequency of backups, and<br>▪ Storage of backup media. | | | | |
| 3. The local IT contingency planning process is coordinated with other related agency- and system-level plans (i.e., continuity of operations plan (COOP), system security plans (SSP), business resumption plans (BRP), critical infrastructure protection (CIP), Occupant Emergency Plans (OEP)). | | | | |
| 4. A clearly defined planning process, with an appointed lead, was established and used in the development of local IT contingency plans. | | | | |
| 5. A business impact analysis (BIA) was conducted which:<br>▪ Identified critical IT resources,<br>▪ Determined disruption impacts and allowable outage times, and<br>▪ Developed recovery priorities. | | | | |
| 6. Recovery strategies provide for the quick and effective restoration of local IT operations following a service disruption. | | | | |
| 7. The recovery strategies for local IT systems address:<br>▪ Backup methods,<br>▪ Use of an alternate site,<br>▪ Equipment replacement,<br>▪ Roles and responsibilities of key persons and recovery teams, and<br>▪ Cost considerations. | | | | |

## *IT Contingency Plan Local Implementation Evaluation Checklist*

| Requirement *(Source: NIST SP 800-34)* | Local Implementation | | | Evaluation/Comments |
|---|---|---|---|---|
| | Full | Partial | Missing | |
| 8. Backup methodologies have been clearly defined, and their performance is supported by detailed, documented processes and procedures. | | | | |
| 9. A strategy has been developed to recover and perform system operations at an alternate facility for an extended period. Further, the alternate site strategy identifies the type of site that will be used (e.g., hot, cold, etc). | | | | |
| 10. The use of a designated alternate site is supported by a contract or memorandum of agreement which documents all elements relevant to the use of the site, especially:<br>▪ Site availability/access priority,<br>▪ Guaranteed level of support,<br>▪ IT compatibility,<br>▪ Security requirements,<br>▪ Staff support, and<br>▪ System requirements satisfied (telecommunications and data, hardware, software, and special system needs. | | | | |
| 11. Alternate site planning provided for:<br>▪ Equipment availability,<br>▪ Data and telecommunication needs, and<br>▪ Transportation of persons, equipment, software, records to the alternate site. | | | | |
| ***Plan – Supporting Information and Tools*** | | | | |
| 12. The local plan is structured/formatted to provide for clarity and ease of use. | | | | |
| 13. Checklists and step-by-step procedures provide quick and clear direction for persons unfamiliar with the plan and/or those responding under the stress of emergency conditions? | | | | |
| 14. A *Concept of Operations* description includes:<br>▪ A system description that includes the system architecture, locations, and important technical considerations (e.g., security measures, connectivity, etc),<br>▪ Identification of key persons in authority, including alternates and a line of succession,<br>▪ Recovery objectives and priorities,<br>▪ Recovery teams established to respond to an emergency, the primary objectives of each team, and team membership, and<br>▪ The roles and responsibilities or key persons and team members. | | | | |

## *IT Contingency Plan Local Implementation Evaluation Checklist*

| Requirement (*Source*: *NIST SP 800-34*) | Local Implementation | | | Evaluation/Comments |
|---|---|---|---|---|
| | Full | Partial | Missing | |
| ***Plan – Notification/Activation Phase*** | | | | |
| 15. Notification procedures support situations in which emergency events occur both with and without notice. | | | | |
| 16. When conditions permit, notification procedures provide for advance warning to responsible teams/persons (e.g., notifying the system administrator to permit orderly shutdown of the system). | | | | |
| 17. Procedures support notification of key persons/recovery team personnel during both business and non-business hours. | | | | |
| 18. Notification procedures provide for the orderly coordination of damage assessment teams and recovery teams, if both types of teams are used. | | | | |
| 19. Notification procedures provide for all methods of contact and communication (e.g., telephone, pager, cell phone, e-mail). | | | | |
| 20. Notification procedures provide for backup in the case of widespread communication failures (e.g., providing addresses and maps to permit in-person notification, the use of radio/TV announcements, web sites, automatic assembly at pre-established meeting locations). | | | | |
| 21. Contact information is readily accessible (e.g., call trees, etc). | | | | |
| 22. Procedures are in place to follow in the event key persons cannot be contacted. For example:<br>▪ Having one or more alternates identified,<br>▪ Defining a clear line of succession, and<br>▪ Calling the next available person on the call tree to ensure notification does not break down. | | | | |
| 23. Procedures provide for notification of external organizations that may be impacted by the event, such as shared interconnected systems. | | | | |
| 24. In the case of interconnected systems, contingency plans include an MOU/MOA or interconnection security agreement that details the responsibilities of each party to the agreement as to damage assessment, recovery, and reconstitution. | | | | |

## *IT Contingency Plan Local Implementation Evaluation Checklist*

| **Requirement *(Source*: *NIST SP 800-34)*** | **Local Implementation** | | | **Evaluation/Comments** |
|---|---|---|---|---|
| | **Full** | **Partial** | **Missing** | |
| 25. Damage assessment procedures provide for a complete and timely review of conditions and assembly of an assessment report that details, as a minimum:<br>▪ Cause of the emergency/disruption,<br>▪ Injuries,<br>▪ Potential for additional disruptions or damage,<br>▪ Area affected,<br>▪ Status of physical infrastructure (e.g., structural integrity of computer room, condition of electric power, telecommunications, and heating, ventilation, and air-conditioning [HVAC]),<br>▪ Inventory and functional status of IT equipment (e.g., fully functional, partially functional, and nonfunctional),<br>▪ Type of damage to IT equipment or data (e.g., water damage, fire and heat, physical impact, and electrical surge),<br>▪ Items to be replaced (e.g., hardware, software, firmware, and supporting materials), and<br>▪ Estimated time to restore normal services. | | | | |
| 26. Procedures detail the type of information that should be relayed to management, assessment teams, and recovery teams. | | | | |
| 27. Plan activation criteria have been established, and criteria are documented in contingency plans and in the agency's policy statement. | | | | |
| 28. Step-by-step procedures for activating the plan are documented. | | | | |
| ***Plan – Recovery Phase*** | | | | |
| 29. Recovery phase procedures include guidance/criteria for determining if recovery will be accomplished at the primary or alternate site. | | | | |
| 30. Recovery phase procedures effectively support implementation and execution of the recovery strategies developed during the planning process. | | | | |
| 31. The contingency plan stipulates a planned level of operational/functional capability that would be restored during the recovery phase. | | | | |
| 32. Recovery actions are documented in a logical and sequential manner to permit timely restoration of systems and infrastructure using the proper technical approach. | | | | |
| 33. The sequence of activities used during the recovery phase are based on allowable outage times established in the BIA. | | | | |

*IT Contingency Plan Local Implementation Evaluation Checklist*

| Requirement *(Source: NIST SP 800-34)* | Local Implementation | | | Evaluation/Comments |
|---|---|---|---|---|
| | Full | Partial | Missing | |
| 34. Recovery procedures provide for effective coordination among the various recovery teams both at designated points in the recovery process, and as actual situations dictate. | | | | |
| 35. Recovery at an alternate site is supported by detailed procedures that cover all the logistical and technical requirements applicable to the relocation and restoration of operations. Further, responsibilities for accomplishing these requirements are clearly assigned to the appropriate teams. | | | | |
| 36. As a minimum, detailed step-by-step recovery procedures are provided to support the following actions:<br>▪ Obtaining authorization to access damaged facilities and/or geographic area,<br>▪ Notifying internal and external business partners associated with the system,<br>▪ Obtaining necessary office supplies and work space,<br>▪ Obtaining and installing necessary hardware components,<br>▪ Obtaining and loading backup media,<br>▪ Restoring critical operating system and application software,<br>▪ Restoring system data,<br>▪ Testing system functionality including security controls,<br>▪ Connecting system to network or other external systems, and<br>▪ Operating alternate site equipment successfully. | | | | |
| ***Plan – Reconstitution Phase*** | | | | |
| 37. Procedures provide for evaluating the condition and usability of the original facility/site, and for documenting the repairs, equipment replacement, infrastructure, and other support required to restore it to use. | | | | |
| 38. Criteria exist to assist management in determining whether to repair or replace the original facility. | | | | |
| 39. Teams responsibilities are defined for repairing or replacing the original facility and for transferring IT operations back from the alternate site. | | | | |

| Requirement *(Source: NIST SP 800-34)* | Local Implementation | | | Evaluation/Comments |
|---|---|---|---|---|
| | Full | Partial | Missing | |
| 40. Detailed step-by-step procedures provide for transferring IT systems from the alternate site back to the original/replacement primary facility, and the following areas are covered, as a minimum:<br>▪ Ensuring adequate infrastructure support, such as electric power, water, telecommunications, security, environmental controls, office equipment, and supplies,<br>▪ Installing system hardware, software, and firmware. This activity should include detailed restoration procedures similar to those followed in the Recovery Phase,<br>▪ Establishing connectivity and interfaces with network components and external systems,<br>▪ Testing system operations to ensure full functionality,<br>▪ Backing up operational data on the contingency system and uploading to restored system,<br>▪ Shutting down the contingency system,<br>▪ Terminating contingency operations,<br>▪ Securing, removing, and/or relocating all sensitive materials at the contingency site,<br>▪ Arranging for recovery personnel to return to the original facility. | | | | |
| ***Plan Appendices*** | | | | |
| 41. The following data is included in the local plan appendices:<br>▪ Contact information for team personnel,<br>▪ Vendor contact information, including offsite storage and alternate site POCs,<br>▪ Standard operating procedures and checklists for system recovery or processes,<br>▪ Equipment and system requirements lists of the hardware, software, firmware, and other resources required to support system operations. Details should be provided for each entry, including model or version number, specifications, and quantity,<br>▪ Vendor SLAs, reciprocal agreements with other organizations, and other vital records,<br>▪ Description of, and directions to, the alternate site, and<br>▪ The BIA, conducted during the planning phases. | | | | |

## *IT Contingency Plan Local Implementation Evaluation Checklist*

| Requirement (*Source*: *NIST SP 800-34*) | Local Implementation | | | Evaluation/Comments |
|---|---|---|---|---|
| | Full | Partial | Missing | |
| ***Plan Testing, Training, and Exercises*** | | | | |
| 42. The type of testing (e.g., tabletop walkthroughs, simulations, war-gaming) that will be performed is clearly defined. | | | | |
| 43. A test plan has been developed that details the:<br>▪ Schedule for testing,<br>▪ Type of testing,<br>▪ Test participants,<br>▪ Test scope,<br>▪ Scenario, and<br>▪ Logistics. | | | | |
| 44. Test objectives and success criteria are established to assist in evaluating test results. | | | | |
| 45. As a minimum, the test scenarios provide coverage of the following areas:<br>▪ Notification procedures,<br>▪ System recovery on an alternate platform from backup media,<br>▪ Coordination among recovery teams,<br>▪ Internal and external connectivity,<br>▪ System performance using alternate equipment, and<br>▪ Restoration of normal operations. | | | | |
| ***Plan Maintenance*** | | | | |
| 46. Maintenance policies and procedures require a review of the contingency plan, for accuracy and completeness, at least annually or whenever significant changes occur to any element of the plan. | | | | |
| 47. At a minimum, plan maintenance reviews focus on the following elements:<br>▪ Operational requirements,<br>▪ Security requirements,<br>▪ Technical procedures,<br>▪ Hardware, software, and other equipment (types, specifications, and amount),<br>▪ Names and contact information of team members,<br>▪ Names and contact information of vendors, including alternate/off-site POCs,<br>▪ Alternate and offsite facility requirements, and<br>▪ Vital records (electronic and hardcopy). | | | | |

## *IT Contingency Plan Local Implementation Evaluation Checklist*

| **Requirement (*Source*: *NIST SP 800-34*)** | **Local Implementation** | | | **Evaluation/Comments** |
|---|---|---|---|---|
| | **Full** | **Partial** | **Missing** | |
| ***Technical Planning Considerations*** | | | | |
| 48. The IT Contingency Plan is specifically tailored to support the local IT infrastructure components, platforms, and configurations. | | | | |
| 49. The following common technical considerations are provided for:<br>▪ Frequency of backup and offsite storage of data, applications, and the operating system,<br>▪ Redundancy of critical system components or capabilities,<br>▪ Documentation of system configurations and requirements,<br>▪ Interoperability between system components and between primary and alternate site equipment to expedite system recovery, and<br>▪ Appropriately sized and configured power management systems and environmental control. | | | | |
| 50. Technical contingency planning considerations specific to the IT systems/platforms (desktops, mainframes, LAN, etc.) in use locally by the agency is adequate. | | | | |